Law and order situation in NCR

933. SHRI N.K. SINGH: Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether it is a fact that law and order has been worsening in some parts of NCR making it difficult for women to perform even the routine chores with police becoming a silent spectator; and

(b) the action Government has taken to restore confidence of the people in the law and order machinery and enable them to perform their day to day work?

THE MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS (SHRIMATI V. RADHIKA SELVI): (a) and (b) As per the Constitution, "Public Order" is a State subject, and it is primarily the responsibility of the State Governments to maintain law and order in their States. The, Central Government, however, monitors law and order situation in the country on a regular basis, and in the process, maintains close contact with State Governments besides sharing information with them. Whenever necessary, advisories are also sent to the State Governments. When necessary, the Central Government, on the request of the State Government (s) also provides assistance in the from of deployment of Central para-military forces to aid States to effectively deal with any specific situation that may arise.

Cyber crimes on rise

†934. SHRI BRIJ BHUSHAN TIWARI: Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether it is a fact that cyber crime is growing very fast in the world;

(b) whether these crimes are on the rise in India too; and

(c) if so, the action being taken by Government for its prevention?

THE MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS (DR. SHAKEEL AHMAD): (a) The National Crime Records Bureau (NCRB), which compiles State-wise data on various crimes in India under the Information Technology Act, 2000 and Indian Penal Code (IPC), does not have any comparable data to comment on the prevailing cyber crime scenario in the world.

(b) As per information compiled by NCRB, during the years 2005, 2006 and 2007, a total of 179, 142 and 217 cases were registered in the country under the Information Technology Act, 2000 and a total of 302, 311 and 339 cases were registered in the country under cyber crime related Sections of the IPC, respectively.

(c) The existing Information Technology Act, 2000 provides for legal framework to prevent cyber crimes. Further, the Act has been amended to include provisions to address computer crimes like phishing, spamming, online frauds and identity theft as also for data protection. The

†Original notice of the question was received in Hindi.

Department of Information Technology (DIT) has set up Resource Centre for Cyber Forensics at the Centre for Development of Advanced Computing (C-DAC), Thiruvanathapuram, which has developed indigenous cyber forensic tools. These tools are now being used by agencies to investigate cyber crime cases. The C-DAC, Thiruvanathapuram also conducts training programmes for law enforcement agencies on these tools. The Indian Computer Emergency Response Team(CERT-In) provides reactive and proactive support to the cyber incidents in the country. It also liaisons with similar agencies worldwide and users of cyber space in the country including Government, public or private and issues alerts, advisories and vulnerability notes. These advisories are also published on the website of CERT-In (http://www.cert-in.org.in). The CERT-In also interacts with cyber users in the country to mitigate such incidents.

Organizations like Police Academies, Central Bureau of Investigation (CBI), Indian Computer Emergency Response Team (CERT-In), Controller of Certifying Authority (CCA), NCRB, Regional Police Computer Training Centres (RPCTCs) etc. also conduct regular training programmes for imparting training to the police officials for preventing cyber crimes in the country. The Department of Information Technology (DIT) has provided grants to Central Bureau of Investigation (CBI) and Kerala Police to set up Cyber forensic labs for investigation of cyber crimes and these labs will also be used for training of police officers. Three Central Forensic Science Laboratories (CFSLs) and three Government Examiners of Questioned Documents Laboratories (GEsQD) under the Directorate of Forensic Science (DFS) are having good facilities for providing forensic analytical support to the investigating agencies to handle cyber crimes through digital evidence. These laboratories under the DFS regularly conduct training programmes throughout the year for the benefit of law enforcement agencies and train them in search and seizure methods for handling cyber crimes and Internet crimes, e-mail investigations, mobile phone forensics etc.. The Government has also conducted several awareness and training programmes on cyber laws and cyber crimes for Judicial officers and Law Enforcement Agencies.

Further, under the Plan Scheme of Eleventh Five Year Plan of the Directorate of Forensic Science (DFS), for improving the facilities and training in handling cases of cyber crime, Information Technology etc. of Directorate of Forensic Science, there is a Scheme titled 'Creation of National Training and Resource Centre for Cyber Forensics', with an outlay of Rs. 10 crore.

Tunnel on Pakistan border in Rajasthan

935. SHRI M. RAMA JOIS: Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether a tunnel has been dug between India and Pakistan International Border, abutting Rajasthan, enabling trespass and for indulging in smuggling activities as reported in the media; and

(b) if so, the steps taken by Government for closing the said tunnel?